

APNIC: Solving problems for our community

Sofía Silva Berenguer

Information Services Product Manager

sofia@apnic.net

A bit about me

- I started my journey in the RIR world working as a Hostmaster and Policy Officer at LACNIC in August 2010
- I then had some technical roles:
 - Networks and Security Engineer
 - Senior Security and Stability Engineer
- I started working with APNIC as a Data Scientist more than 2 years ago
- I've always suffered from Impostor Syndrome



Agenda

- Information Services Product family:
 - DASH (Dashboard for Autonomous System Health)
 - NetOX (Network Operators tool boX)

DASH (Dashboard for AS Health)

- Dashboard for resource holders that shows **information about malicious traffic** seen by our honeypots originated at IP addresses managed by the user
- Currently just a prototype:
 - Only showing information about SSH attacks
 - More features pending to be implemented
- Short video available: <https://dash.apnic.net/about>
- Preparing soft launch with set of Members who would find interesting info in the current version of the product

DASH

- My dashboard
- IPv4 prefixes
- IPv6 prefixes
- Latest security news

Useful Links

- About

testaccount ▾ testASN ▾

My dashboard

This Month ▾ [Generate Report](#)

My network

Total attacks in JUL
2.1K

Compared to previous month
↑ 0.3%

Total attacks in JUN
2.1K

VN

Total attacks in JUL
17.3K

Compared to previous month
↓ 28.3%

Total attacks in JUN
24.1K

South-Eastern Asia

Total attacks in JUL
23.3K

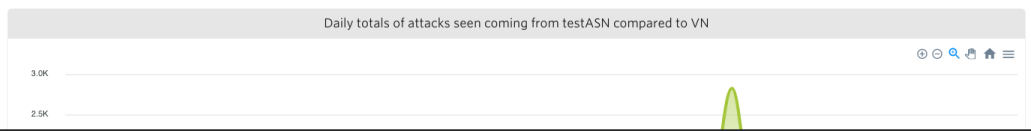
Compared to previous month
↓ 15.0%

Total attacks in JUN
27.5K

Feedback
😊

Number of attacks seen from my network compared to VN

[VN](#) [South-Eastern Asia](#)



DASH

testaccount testASN

- My dashboard
- IPv4 prefixes
- IPv6 prefixes
- Latest security news

Useful Links

About

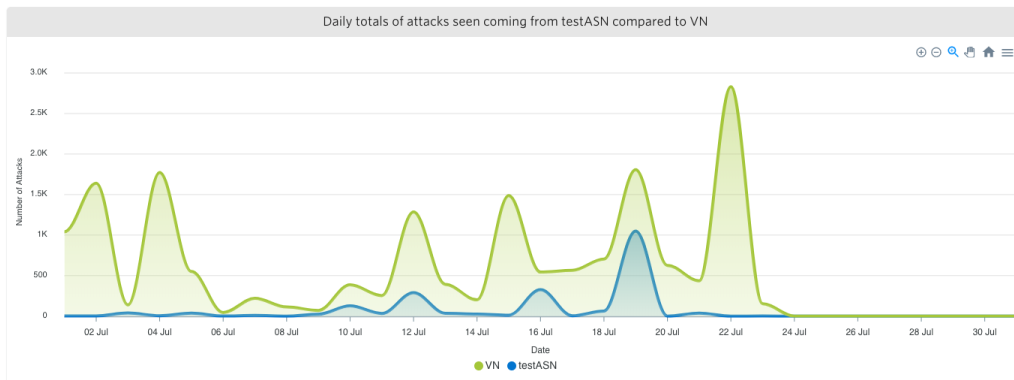
My dashboard

This Month

Generate Report

Number of attacks seen from my network compared to VN

VN South-Eastern Asia



Feedback

DASH

- My dashboard
- IPv4 prefixes
- IPv6 prefixes
- Latest security news

Useful Links

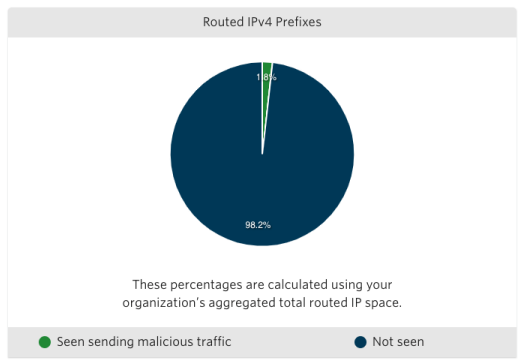
- About

testaccount ▾ testASN ▾

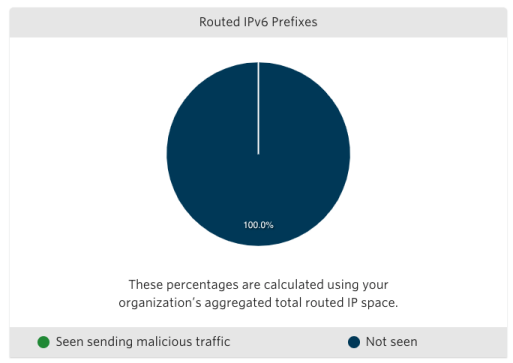
My dashboard

This Month ▾ [Generate Report](#)

Overview of my routed prefixes



[View my offending IPv4 prefixes](#)



[View my offending IPv6 prefixes](#)

Feedback
😊

My dashboard

This Month Generate Report

My network top 10 offending prefixes

| Prefix | Attack types | Count |
|-----------------|--------------|-------|
| 198.51.100.0/24 | SSH | 1055 |
| 10.183.93.0/24 | SSH | 683 |
| 10.118.0.0/20 | SSH | 135 |
| 192.0.2.0/20 | SSH | 63 |
| 198.51.100.0/20 | SSH | 57 |
| 10.210.0.0/21 | SSH | 35 |
| 10.118.16.0/20 | SSH | 18 |
| 10.210.112.0/21 | SSH | 13 |
| 10.118.32.0/20 | SSH | 10 |
| 10.74.120.0/22 | SSH | 6 |



Feedback



DASH – Use Case

I've received an alert from APNIC DASH: 20 % of my IPv4 addresses have been seen sending malicious traffic!

It seems two of the networks we use for corporate customers may have devices infected with malware. I'll talk to them to get their networks checked.

I better check which prefixes may be compromised.

(Logs in to DASH)

Top 10 offending prefixes (This Month)

| Prefix | Attack | Count |
|-----------------|--------|-------|
| 203.0.113.0/24 | SSH | 110 |
| 198.51.100.0/24 | SSH | 105 |



Yoshi
"I run the net"

NetOX (Network Operators ToolbOX)

- Set of tools that helps network operators interact with other networks
 - Solving routing issues
 - Deciding which other networks to connect to
- Working in collaboration with the RIPE NCC
- Currently RIPEstat with an APNIC ‘look & feel’
- Available at: <https://netox.apnic.net>

Search Internet Number Resources

This is APNIC's Network Operators ToolbOX, powered by RIPE NCC's RIPEstat. It is currently just a prototype. If you have any questions or comments, please reach out to us at feedback@apnic.net



AS Overview (AS4608)

Routing information (RIS)

- Originates prefixes visible
- Is seen in other routes

Name and holder of this ASN:

APNIC-SERVICES Asia Pacific Network Information Centre

| RIR | Status | Registration | Country |
|-------|-----------|--------------|---------|
| APNIC | ALLOCATED | 1995-05-30 | AU |

Show IANA Registry Information

Showing results for AS4608 as of 2019-05-19 16:00:00 UTC

Whois Matches (AS4608)

Whois results (1)

Show more fields

| | |
|---------|--|
| aut-num | 4608 |
| as-name | APNIC-SERVICES |
| descr | Asia Pacific Network Information Centre |
| descr | Regional Internet Registry for the Asia-Pacific Region |
| descr | 6 Cordelia Street |
| descr | PO Box 3646 |
| descr | South Brisbane, QLD 4101 |
| descr | Australia |
| country | AU |
| org | ORG-APNII-AP |
| mnt-by | APNIC-HM |

Routing registries results (0)

Showing results for AS4608 as of 2019-05-20 01:35:00 UTC

NetOX in the future

- Exploring how to implement features to solve validated problems:
 - Bringing points of contact and other data (?) from PeeringDB
 - Easily visualizing upstream providers for a given ASN
 - Bringing data from IRRs, for automation of route filters
- Exploring idea of creating shared knowledge base for network operators

NetOX – Use Case

I'm considering hiring a new upstream provider. I wonder how well interconnected AS 4608 is??

They probably offer good robustness as they have three providers.



Yoshi
"I run the net"

Peers and Providers (AS4608)


Show entries Search:

| ASN | Name | Type |
|---------|---------------------------|----------|
| AS42 | WOODYNET-1 - WoodyNet | peer |
| AS714 | APPLE-ENGINEERING - Ap... | peer |
| AS1221 | ASN-TELSTRA Telstra Co... | provider |
| AS3303 | SWISSCOM - Swisscom (S... | peer |
| AS7575 | AARNET-AS-AP Australia... | provider |
| AS24130 | TPG-AU TPG Internet Pt... | provider |

Showing 1 to 6 of 6 entries

ASN names are valid for 2019-07-01 08:25 UTC
The CAIDA AS Relationships Dataset, 2019-06-01. <https://www.caida.org/data/as-relationships/>

NetOX – Use Case



I'm having some routing issues. AS 4608 seems to be filtering one of my prefixes.

I've tried contacting the WHOIS PoC but they were not very responsive.

There must be a better contact for this type of issue.

Peeringdb contacts (AS4608)

Contact info

| Name | Role | Email | Phone |
|-------------------------|-----------|-------------------|---------------|
| Infrastructure Services | Technical | peering@apnic.net | +617 38583100 |
| Network Operations | NOC | noc@apnic.net | +617 38583100 |

Yoshi
"I run the net"

NetOX – Use Case

I'm getting 27.100.7.0/24 transferred. I wonder if this prefix is clean.

It looks like this prefix is already in use!

And it has been routed for quite a long time!



Yoshi
"I run the net"

Search Internet Number Resources

This is APNIC's Network Operators ToolBox, powered by RIPE NCC's RIFEstat. It is currently just a prototype. If you have any questions or comments, please get in touch with Sofia at sofia@apnic.net

27.100.7.0/24

At a Glance Routing DNS Anti Abuse Database Geographic **RQA** Activity

Routing Status (27.100.7.0/24)

At 2019-07-01 00:00:00 UTC, 27.100.7.0/24 was 100% visible (by 237 of 237 RIS full peers).

First ever seen announced by AS56096, on 2013-10-13 00:00:00 UTC.

Originated by:
AS56096 - RPKI Status: - Route objects: RADB and NTTCOM
No less-specific covering prefixes.

Showing results for 27.100.7.0/24 as of 2019-07-01 00:00:00 UTC

Results exclude routes with very low visibility (less than 10 RIS full-peer seeding).

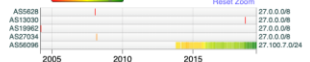
Routing History (27.100.7.0/24)

Switch to Table View

Show all of 16 rows Sort by 123 Condensed view

Filters (1): No large prefixes No short timespans No low visibility

Data resolution: 12 days

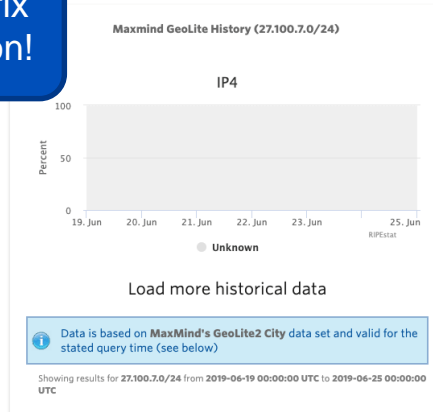


Showing results for 27.100.7.0/24 from 2000-08-01 00:00:00 UTC to 2019-07-01 00:00:00 UTC

NetOX – Use Case

Uhhmm It hasn't been assigned by APNIC yet.

This prefix is a bogon!



Whois Matches (27.100.7.0/24)

Whois results (1) [Show more fields](#)

| | |
|---------|--|
| inetnum | 27.0.0.0/8 |
| netname | APNIC-AP |
| descr | Asia Pacific Network Information Centre |
| descr | Regional Internet Registry for the Asia-Pacific Region |
| descr | 6 Cordelia Street |
| descr | PO Box 3646 |
| descr | South Brisbane, QLD 4101 |
| descr | Australia |
| country | AU |
| mnt-by | APNIC-HM |
| status | ALLOCATED PORTABLE |
| source | APNIC |

Routing registries results (6)

Showing results for 27.100.7.0/24 as of 2019-07-01 06:19:00 UTC

Yoshi
"I run the net"

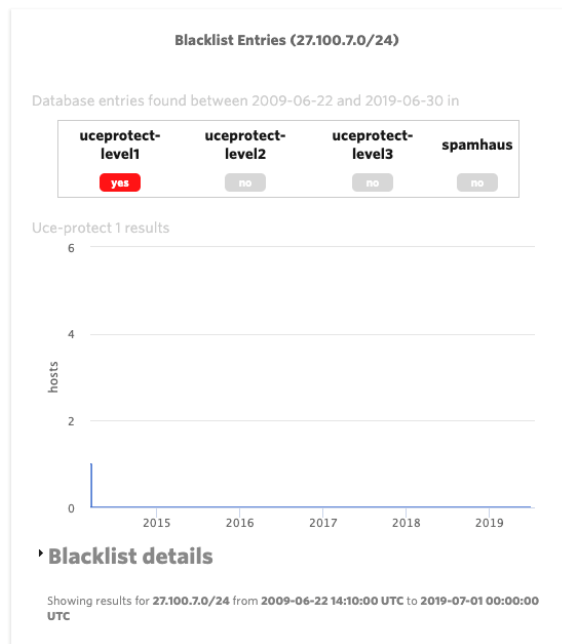
NetOX – Use Case

And it's in a black list!

This prefix is definitely not clean!



Yoshi
"I run the net"



Summary

- We are working on products to offer info to network operators
 - **DASH** (Dashboard for AS Health)
 - **NetOX (Network Operators toolboX)**
- We want to hear **FROM YOU!**
 - Do you see value in these products?
 - Do you want to provide any feedback?
 - Do you want to participate in interviews, testing sessions, etc.?

THANK YOU